CLAIMS

What is claimed is:

1	1.	A me	thod for booting up a computer system in a secure fashion comprising the steps
2	of:		
3		a)	determining the presence of a security feature element during an initialization
4	of the	e-compu	ter system wherein the security feature element includes a public key and a
5	corre	spondin	g private key;
6		b)	storing a portion of the public key in a nonvolatile memory within the
7	comp	outer sys	tem if the security feature element is present; and
8		c)	utilizing an algorithm to determine the presence of the security feature
9	eleme	ent prior	to a subsequent boot-up of the computer system.
1	2	The m	nethod of claim 1 wherein the security feature element comprises a security
1	2.	i ne n	lethod of claim? Wherein the security reature element comprises a security
2	card.		
1	3.	The m	nethod of claim 2 wherein the security card provides for tamper detection of the
2	comp	uter sys	tem and the security card, temperature monitoring of the computer system and
3	volta	ge status	s reporting of the computer system.

The method of claim 1 wherein step c) is performed during a Power-On-Self-Test

(POST) sequence.

4.

1

1	5.	The method of claim 4 wherein step c) further comprises:		
2		c1) determining the presence of the security card.		
1	6.	The method of claim 5 wherein step c1) further comprises:		
2		c1a) determining if the computer system has been subjected to a tamper event if		
3	the s	ecurity card is present.		
		and the state of t		
1	7.	The method of claim 6 wherein step c1) further comprises:		
2		c1a) determining whether a security card was previously present in the computer		
3 .	syste	m if the security card is not present.		
1	8.	The method of claim 7 wherein step c1) further comprises:		
2		c1b) clearing the portion of the public key stored in the non-volatile memory of		
3	the co	he computer system if a security card was previously present in the computer system; and		
4		clc) prompting for an authorization prior to booting up the computer system.		
1	9.	The method of claim 7 wherein step c1) further comprises:		
2		clb) booting up the computer system if the security card was not previously		
3	prese	nt in the computer system.		
1	10.	The method of claim 6 wherein step c1) further comprises:		
2		clb) booting up the computer system if the computer system has not been		
3	subje	cted to a tamper event.		

2

3

1	11.	The method of claim 6 wherein step c1) further comprises:
2		c1b) determining whether the security card is an added feature of the computer
3	syster	n, wherein the determination is based on a previous POST sequence, if the computer
4	syster	n has been subjected to a tamper event.
1	12.	The method of claim 11 wherein step c1) further comprises:
2		_c1c) clearing the portion of the public key stored in the nonvolatile memory of the
3	comp	uter system if the card is a newly added feature of the computer system; and
4		c1d) prompting for an authorization prior to booting up the computer system.
1	13.	The method of claim 11 wherein step c1) further comprises:
2		c1c) comparing the public key on the security card with the portion of the public
3	key st	ored in the nonvolatile memory of the computer system if the security card is not a
4	newly	added feature of the computer system.
1	14.	The method of claim 13 wherein step c1) further comprises:
2		cld) booting up the computer system if the public key on the security card
3	match	nes the portion of the public key stored in the nonvolatile memory of the computer
4	syster	n.
1	15.	The method of claim 13 wherein step c1) further comprises:
2		cld) clearing the portion of the public key stored in the nonvolatile memory of the

computer system;

4		cle)	clearing the public key and the corresponding private key stored on the
5	security card; and		
6		clf)	booting up the computer system.
1 ·	16.	A syste	em for booting up a computer in a secure fashion, the system comprising:
2		means	for determining the presence of a security feature element during an .
3	initialization of the computer system wherein the security feature element includes a public		
4	key and a corresponding private key;		
5	÷	means	for storing a portion of the public key in a nonvolatile memory within the
6	compu	iter syst	em if the security feature element is present; and
7		means	for utilizing an algorithm to determine the presence of the security feature
8	elemer	nt prior	to a subsequent boot-up of the computer system.
1	17.	The sy	stem of claim 16 wherein the security feature element comprises a security
2	card.		
1	18.	The sy	stem of claim 17 wherein the security card provides for tamper detection of
2	the cor	nputer a	and the security card, temperature monitoring of the computer and voltage
3	status	reportin	g of the computer.
1	19.	The sy	stem of claim 18 wherein the algorithm is utilized during a Power-On-Self-
2	Test (F	POST) s	equence.

1	20.	The system of claim 19 wherein the means for utilizing the algorithm further				
2	comp	comprises:				
3		means for determining the presence of the security card.				
1	21.	The system of claim 20 wherein the means for utilizing the algorithm further				
2	comp	comprises:				
3		means for determining if the computer has been subjected to a tamper event if the				
4	secur	ity card is present.				
1	22.	The system of claim 20 wherein means for utilizing the algorithm further comprises:				
2		means for determining whether a security card was previously present in the				
3	comp	uter if the security card is not present.				
1	23.	The system of claim 22 wherein the means for determining the presence of the				
2	secur	ity card further comprises:				
3		means for clearing the portion of the public key stored in the non-volatile memory of				
4	the co	omputer if a security card was previously present in the computer; and				
5		means for prompting for an authorization prior to booting up the computer.				
1	24.	The system of claim 22 wherein the means for determining the presence of the				
2	securi	ity card further comprises:				
3		means for booting up the security system if the security card was not previously				
4	preser	nt in the computer.				

5

1	25.	The system of claim 21 wherein the means for determining the presence of the	
2	security card further comprises:		
3		means for booting up the computer if the computer has not been subjected to a	
4	tamper	event.	
•			
1	26.	The system of claim 21 wherein the means for determining the presence of the	
2	securit	y card further comprises:	
3		means for determining whether the card is a newly added feature of the computer,	
4	wherei	n the determination is based on a previous POST sequence, if the computer has been	
5	subject	ed to a tamper event.	
1	27.	The system of claim 26 wherein the means for determining the presence of the	
2	securit	y card further comprises:	
3		means for clearing the portion of the public key stored in the nonvolatile memory of	
4	the cor	nputer if the card is a newly added feature of the computer; and	
5		means for prompting for an authorization prior to booting up the computer.	
1	28.	The system of claim 26 wherein the means for determining the presence of the	
2	securit	y card further comprises:	
3		means for comparing the public key on the security card with the portion of public	
4	key sto	red in the nonvolatile memory of the computer if the security card is not a newly	

added feature of the computer.

1	29.	The system of claim 28 wherein the means for determining the presence of the
2	securi	ty card further comprises:
3		means for booting up the computer system if the public key on the security card
4	match	es the portion of the public key stored in the nonvolatile memory of the computer.
1	30.	The system of claim 28 wherein the means for determining the presence of the.
2	securi	ty card further comprises:
3		means for clearing the portion of the public key stored in the nonvolatile memory of
4	the co	mputer;
5		means for clearing the public key and the corresponding private key stored on the
6	securi	ty card; and
7		means for prompting for an authorization prior to booting up the computer.